A SELF CONTAINED GUIDE TO SQUARE SIEVES AND APPLICATIONS

NAVVYE ANAND

Abstract. Sieves have been an important part of number-theory for over a century. In this expository paper, we discuss a specific type of sieve called the **square sieve**, and discuss its various applications with respect to elliptic curves and other number-theoretic objects.

1. Introduction to sieves

What exactly are sieves? Well, a sieve is a technique used in number theory to count, or estimate the size of a given set of integers. sieve theory is used to obtain suitable (non-trivial) bounds on cardinality of sets with a particular property, usually related to primes or squares. sieves have proven to be invaluable tools in number theory. We also note the following typical questions which involve sieve theory:

(1) Is every even integer $n \geq 2$ a sum of two primes? (Goldbach's conjecture)
(2) Are there infinitely many pairs of primes (p, q) with $q = p + 2$? (the twin primes conjecture)
(3) Are there arbitrary long arithmetic progressions consisting only of primes?
(4) Are there infinitely many primes of the form $n^2 + 1$ with $n \in \mathbb{N}$?
(5) Is it true that, for every $n \in \mathbb{N}$, there is a prime p in the range $n^2 < p < (n+1)^2$?
(6) For every $\varepsilon > 0$ is there an integer $N(\varepsilon)$ such that the interval $[N, N + N^\varepsilon]$ contains a square-free number, as soon as $N \geq N(\varepsilon)$?

1.1. Sieve of Eratosthenes.

Perhaps the most famous example of any sieve is perhaps the so called **sieve of Eratosthenes**, which is used to generate prime numbers. The algorithm for implementing the **sieve of Eratosthenes** is shown below.

---

(1) Create a list of consecutive integers from 2 through n: (2, 3, 4, . . . , n).
(2) Initially, let p equal 2, the smallest prime number.
(3) Enumerate the multiples of p by counting in increments of p from $2p$ to n, and mark them in the list (these will be $2p, 3p, 4p, \ldots$; the p itself should not be marked).
(4) Find the smallest number in the list greater than p that is not marked. If there was no such number, stop. Otherwise, let p now equal this new number (which is the next prime), and repeat from step 3.
(5) When the algorithm terminates, the numbers remaining not marked in the list are all the primes below n.

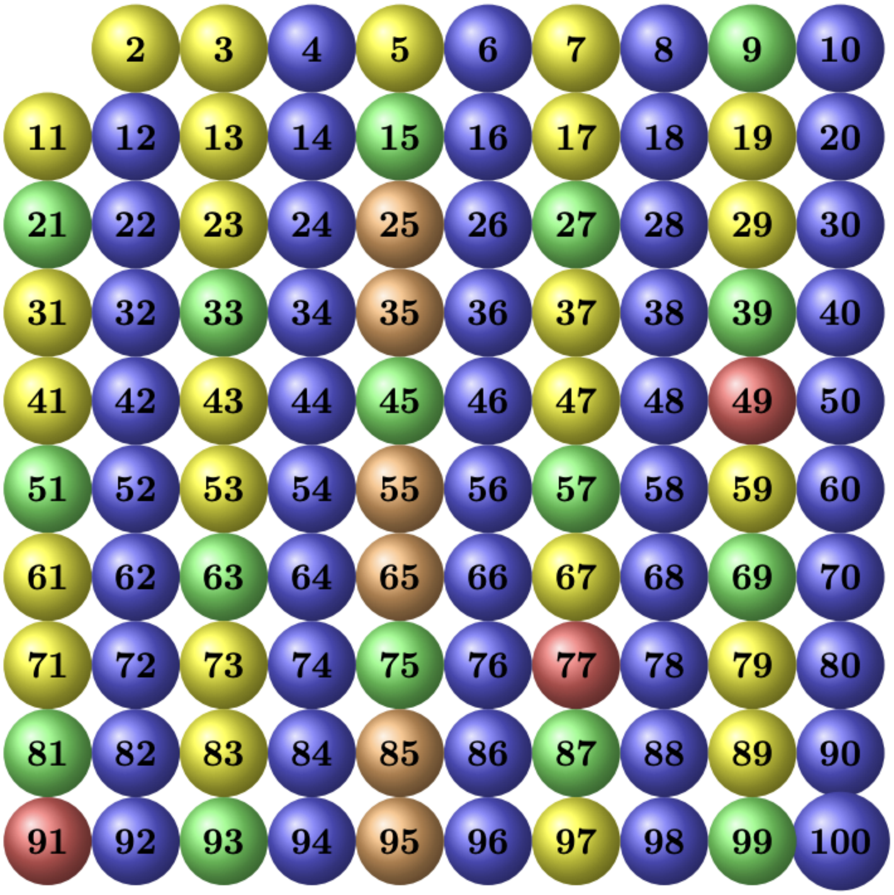

Figure 1. sieve of Eratosthenes

Now that we have looked at an example of a 'sieve', we shall discuss precursory sieves, which will lead us to the square sieve.

2. Precursory sieves

2.1. **Gallagher's sieve [1].** We begin by noting Linnik's large sieve which gives an upper bound for the number of integers which remain in an interval of length N after $f(p)$ different residue classes modulo p have been removed for $p \in \mathcal{P}$. Gallagher notes the following upper bound exists for an absolute constant C.

$$\frac{N + CQ^2}{S(Q)} \quad \text{where} \quad S(Q) = \prod_{q \leq Q} \mu^2(q) \prod_{p|q} \frac{f(p)}{p - f(p)}. \tag{2.1}$$

Gallagher notes that in some cases, 2.1 is best possible. As an example of this, we consider the case when all quadratic non-residues modulo p are removed for each prime p. Therefore, the perfect squares remain. Since $f(p) = \frac{p-1}{2}$, this implies that $S(Q) \gg Q$ and thus the upper bound is $\ll N^{1/2}$ for $Q = N^{1/2}$. However, the bound is not optimal, especially when $f(p)$ is close to p, and therefore Gallagher introduces a *sieve* to get a better result.

Theorem 2.1 (Gallagher's sieve). *Set $g(p) = p - f(p)$. If all but $g(q)$ residue classes modulo q are removed for each prime power q in a finite set $\mathcal{P}$, then the number of integers which remain in any interval of length N is at most*

$$\left(\sum_{q\in\mathcal{P}} \Lambda(g) - \log(N)\right) / \left(\sum_{q\in\mathcal{P}} \frac{\Lambda(q)}{g(q)} - \log(N)\right)$$

where $\Lambda(q) = \log(p)$ for $q = p^\alpha$ and $g(q) > 0$.

Proof. Assume Z integers modulo n remain in a given interval of length N and $Z(h,q)$ of these satisfy $n \equiv h \pmod{q}$, then

$$Z^2 = \left(\sum_{h=1}^{q} Z(h,q)\right)^2 \leq g(q)\sum_{h=1}^{q}(Z(h,q))^2.$$

Now, since $q \in \mathcal{P}$, we have $Z(h,q) = 0$ for all but $g(q)$ values of h. Summing over $\mathcal{P}$, we get

$$Z^2 \sum_{q\in\mathcal{P}} \frac{\Lambda(q)}{g(q)} \leq \sum_{q\in\mathcal{P}} \Lambda(g) \sum_{m\equiv n(q)} 1 = \sum_{|d|\leq N} \left(\sum_{m-n=d} 1\right)\left(\sum_{q|d,q\in\mathcal{P}} \Lambda(q)\right) \leq Z\sum_{q\in\mathcal{P}} \Lambda(q) + (Z^2 - Z)\log(N).$$

Finally, the fact that $\sum_{q|d} \Lambda(q) = \log(|d|)$ implies 2.1. ■

We also obtain the following corollary.

Corollary 2.2. *If all but G residue classes modulo q have been removed for each $q \in \mathcal{P}$, then the number of integers which remain in any interval of length N is at most*

(1)

$$\leq G \quad \textit{if} \quad \sum_{q\in\mathcal{P}} \Lambda(q) > G^2\log(N)$$

(2)

$$\leq 2G - 1 \quad \textit{if} \quad \sum_{q\in\mathcal{P}} \Lambda(q) \geq 2G\log(N)$$

Proof. 2.1 tells us that

$$Z \leq \frac{L - l}{L/G - l} = G + \frac{G^2 L - Gl}{L - Gl} \quad (L > Gl).$$

If $L > G^2 l$, then $Z \leq G + 1$. We may assume G is an integer, so this implies $Z \leq G$. If $L \geq 2Gl$, we get $Z \leq 2G - 1$.

■

The upper bound given above is certainly best possible since any G different integers will represent $\leq G$ different residue classes (mod q), for every q. The condition $L > G^2 l$ in the corollary is also best possible if $G = 1$. For example, if N is a square-free positive integer and $\mathcal{P}$ is the set of prime divisors of N, then $L = l$, while the two integers 0 and N represent only the zero class (mod p) for each $p \in \mathcal{P}$. Now, we turn our attention towards another family of sieves introduced by Montgomery and Davenport.

2.2. **Montgomery and Davenport's sieve [2], [3].** We begin by noting that Montgomery and Davenport's sieve requires more background as compared to Gallagher's sieve because of its analytic nature. Therefore, we begin by describing the pre-requisite inequalities required to set-up the sieve.

2.2.1. *Pre-requisite Inequalities.*

Theorem 2.3 (Sobolev-Gallagher)**.** *Let $a < b$ where $(a,b) \in \mathbb{R}^2$ and f be a continuous complex-valued function on $[a,b]$ with continuous first derivative in (a,b). Then,*

$$\left| f\left(\frac{a+b}{2}\right) \right| \leq \frac{1}{b-a}\int_a^b |f(x)|\,\mathrm{d}x + \frac{1}{2}\int_a^b |f'(x)|\,\mathrm{d}x$$

and

$$|f(u)| \leq \frac{1}{b-a}\int_a^b |f(x)|\,\mathrm{d}x + \int_a^b |f'(x)|\,\mathrm{d}x$$

for any $u \in [a,b]$

Now, by applying 2.3 repeatedly, we get the following lemma.

Lemma 2.4. *Let T_0 and $T \geq \delta \geq 0$ be real numbers, and let f be a continuous complex-valued function on the interval $[T, T+T_0]$ with continuous derivative in $(T, T+T_0)$. Now, let $\mathcal{J}$ be a set of real numbers in the interval $\left[T_0 + \frac{\delta}{2}, T_0 + T - \frac{\delta}{2}\right]$, and suppose that $|t - t'| \geq \delta$ for distinct $t, t' \in \mathcal{J}$. Then,*

$$\sum_{t \in \mathcal{J}} |f(t)| \leq \frac{1}{\delta}\int_{T_0}^{T+T_0} |f(x)|\mathrm{d}x + \frac{1}{2}\int_{T_0}^{T+T_0} |f'(x)|\mathrm{d}x.$$

Lemma 2.5. *Let $T_0, T \geq \delta \geq 0$ be real numbers and let $\mathcal{J}$ be a finite set in the interval $[T_0 + \frac{\delta}{2}, T_0 + T - \frac{\delta}{2}]$. Define $N_\eta(x) = \sum_{t \in \mathcal{J}, |t-x|<\eta} 1$. Then, for f defined in 2.4 and $\eta > 0$, we have*

$$\sum_{t \in \mathcal{J}} |f(t)| \cdot N_\delta(t)^{-1} \leq \frac{1}{\delta}\int_{T_0}^{T_0+T} |f(x)|\mathrm{d}x + \frac{1}{2}\int_{T_0}^{T+T_0} |f'(x)|\mathrm{d}x.$$

By setting $f(t) = S(t)^2$, we get $f'(t) = 2S(t)S'(t)$. Now, from the above-mentioned inequality and by utilizing Cauchy-Schwarz, we get the following lemma from Gallagher.

Lemma 2.6 (Gallagher)**.** *Let $T_0, T, \delta, \mathcal{J}$ and $N_\delta(t)$ be defined as above. Then, suppose S is a continuous complex valued function in the interval $[T, T_0 + T]$, with a continuous derivative in $(T, T_0 + T)$. Then,*

$$\sum_{t \in \mathcal{J}} N_\delta(t)^{-1}|S(t)|^2 \leq \frac{1}{\delta}\int_{T_0}^{T+T_0} |S(t)^2|\mathrm{d}t + \sqrt{\int_{T_0}^{T+T_0} |S(t)|^2\mathrm{d}t \cdot \int_{T_0}^{T+T_0} |S'(t)|^2\mathrm{d}t}.$$

Now that we have looked at analytic sieves, we turn our attention towards generalizations of Bessel's inequality for vectors in an inner-space product. As a reminder, Bessel's inequality is stated below.

Lemma 2.7 (Bessel's Inequality)**.** *Let $\varphi_1, \varphi_2, \cdots, \varphi_r$ be a sequence of orthonormal elements of an inner product space over the complex numbers, then for some ζ, the following inequality holds*

$$\sum_{r=1}^{R} |(\zeta, \varphi_r)|^2 \leq \|\zeta\|^2.$$

Furthermore, if $R = 1$, we have

$$|(\zeta, \varrho)| \leq \|\zeta\| \|\varrho\|$$

for any ζ, ϱ.

We desire an inequality that works even when $\varphi_1, \varphi_2, \cdots, \varphi_r$ are not orthonormal. The following lemma which was discovered by Boas does exactly that!

Lemma 2.8. *The inequality*

$$\sum_{r=1}^{R} |(\zeta, \varphi_r)|^2 \leq \|\zeta\| \left(\max{}_{1\leq r\leq R} \|\varphi_r\| + \left(\sum_{r\neq s} |(\varphi_r, \varphi_s)|^2 \right)^{1/2} \right)$$

holds for any $\varphi_1, \varphi_2, \cdots, \varphi_r$.

Bombieri stated the following lemma, which is a variation of 2.8.

Lemma 2.9 (Bombieri)**.** *If $\zeta, \varphi_1, \varphi_2, \cdots, \varphi_r$ are elements of an inner product space over the complex numbers then*

$$\sum_{r=1}^{R} |(\zeta, \varphi_r)|^2 \leq \|\zeta\|^2 \left(\max{}_{1\leq r\leq R} \sum_{r=1}^{R} |(\varphi_r, \varphi_s)| \right).$$

Selberg found a stronger result independently of Bombieri, which is stated below.

Lemma 2.10 (Selberg)**.** *If $\zeta, \varphi_1, \varphi_2, \cdots, \varphi_r$ are elements of an inner product space over the complex numbers then*

$$\sum_{r=1}^{R} |(\zeta, \varphi_r)|^2 \cdot \left(\sum_{s=1}^{R} |(\varphi_r, \varphi_s)| \right)^{-1} \leq \|\zeta\|^2$$

We now circle back to Gallagher's theorems, in particular, we state a generalization of Gallagher's sieve. Then, the following lemma holds.

Lemma 2.11. *Let $S(t) = \sum_{\mu\in\mathcal{M}} c(\mu)e(\mu t)$ where $e(x) = e^{2\pi i x}$, $\mathcal{M}$ is a countable set of real numbers, and $c(\mu)$ is a sequence of real or complex numbers subject to the condition that $\sum_{\mu} c(\mu) < \infty$, then for any $\varepsilon > 0$, if δ, T are positive real numbers satisfying the inequality $\delta T \leq 1 - \varepsilon$, then*

$$\int_{-T}^{T} |S(t)|^2 \mathrm{d}t \ll_{\varepsilon} \int_{-\infty}^{\infty} |C_\delta(x)|^2 \mathrm{d}x$$

where

$$C_\delta(x) = \delta^{-1} \sum_{|\mu - x| < \delta/2} c(\mu).$$

The above-mentioned theorem can be generalized in context of Dirichlet series as follows.

Lemma 2.12. *Define* $S(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$ *to be absolutely convergent for* $\mathrm{Re}(s) > 0$*, then*

$$\int_{-T}^{T} |S(it)|^2 \mathrm{d}t \ll T^2 \int_0^{\infty} \left| \sum_{y}^{\tau y} a_n \right|^2 \frac{\mathrm{d}y}{y}$$

where $\tau = \exp(T^{-1})$ *and* $T > 0$*.*

With that, we conclude the pre-requisite inequalities and move on to the main portion of Montgomery and Davenport's sieve.

2.2.2. *Main Sieve.* Our main goal in this section is to find a bound an upper bound for $\sum_{x \in \mathcal{X}} S(x)$, where $\mathcal{X}$ is a sequence of real numbers well-spaced modulo 1, and $S(x)$ is an arbitrary exponential polynomial, defined as $S(x) := \sum_{n=M+1}^{M+N} a_n e(nx)$ with $e(x) = e^{2\pi i x}$. Now, from 2.6, we immediately have the following theorem.

Theorem 2.13 (Davenport Sieve)**.** *Define* $S(x)$ *as above. Then, if* $\mathcal{X}$ *is a set of real numbers in* $(0, 1]$*, then if* $0 < \delta < \frac{1}{2}$*, then*

$$\sum_{x \in \mathcal{X}} N_\delta(x)^{-1} |S(x)|^2 \le (\delta^{-1} + \pi N) \sum_n |a_n|^2,$$

where

$$N_\delta(y) = \sum_{\substack{x \in \mathcal{X} \\ \|x - y\| < \delta}} 1.$$

Davenport gave an explicit version of the sieve mentioned above, with the assumption that $\delta \le \frac{1}{4N}$. We now state a useful corollary discovered by Gallagher.

Corollary 2.14 (Gallagher)**.** *If* $S(x)$ *is defined as above, and* $\mathcal{X}$*, is a set of real numbers for which* $\|x - x'\| \ge \delta > 0$*, wherever* x *and* x' *are distinct members of* $\mathcal{X}$*, then*

$$\sum_{x \in \mathcal{X}} |S(x)|^2 \le \left(\delta^{-1} + \pi N\right) \sum_n |a_n|^2.$$

Furthermore, if $x \in \mathcal{X}$ *are equally spaced* $\pmod 1$*, then* $\delta \sum |S(x)|^2$ *is a Riemann sum approximating to*

$$\int_0^1 |S(x)|^2 \mathrm{d}x = \sum |a_n|^2.$$

Theorem 2.15 (Large Sieve Inequality)**.** *Let* X *be a finite set of points of* $\mathbb{R}/\mathbb{Z}$*. Set*

$$\delta = \min\{\|x - x'\|, x \ne x' \in X\}.$$

For any sequence of complex numbers $(u_n)_{1 \le n \le N}$*, we have*

$$\sum_{x \in X} \left| \sum_n u_n e(nx) \right|^2 \le \sum_n |u_n|^2 (N - 1 + \delta^{-1}).$$

3. Heath-Brown's Square Sieve

Let $\mathcal{A}$ be a sequence of integers. Suppose we have information about the distribution of $\mathcal{A}$ with respect to certain moduli. How many squares can $\mathcal{A}$ contain? This problem lies at the heart of Heath-Brown's [4] seminal 1984 paper. In order to formulate the above-mentioned problem *rigorously*, let $\omega(n) \geq 0$ for each $n \in \mathbb{Z}$, and suppose $\sum_{i=1}^{\infty} \omega(i) < \infty$. Writing $\mathcal{A}$ for the sequence $\omega(n)$, we define $S(\mathcal{A}) = \sum_{n=1}^{\infty} \omega(n^2)$. We now introduce Heath-Brown's non-trivial bound on $S(\mathcal{A})$.

Theorem 3.1. *Let $\mathcal{P}$ be a set of P primes. Suppose that $\omega(n) = 0$ for $n = 0$ or $|n| \geq e^P$. Then*

$$S(\mathcal{A}) \ll P^{-1} \sum_n \omega(n) + P^{-2} \sum_{\substack{p \neq q \\ p,q \in \mathcal{P}}} \left(\sum_n \omega(n) \left(\frac{n}{pq} \right) \right),$$

where $\left(\dfrac{n}{pq} \right)$ is the Jacobi symbol.

The attentive amongst the readers would have noticed the fact that Heath-Brown's theorem has an additional side condition. We show that this side-condition is necessary.
Firstly, we note that if $p \mid n$ for some fixed $n > 0$, and for all $p \in \mathcal{P}$, and $\omega(n^2) = 1, \omega(m) = 0$ for $m \neq n$, then $S(\mathcal{A}) = 1$, but the left hand side of the theorem is $O\left(P^{-1}\right)$, making the bound weak by $\log(P)$ factors at least. For an example, we consider $\omega(n) = 1$ for $1 \leq n \leq x$, and $\omega(n) = 0$ otherwise. Now, let $\mathcal{P}$ be the set of primes less than or equal to $x^{1/2}$. Then, using the Polya-Vinogradov inequality, we get

$$\sum_n \omega(n) \left(\frac{n}{pq} \right) \ll x^{1/2} \log(x).$$

Now, we note that the right hand side of the equation is actually $O(x^{1/2} \log x)$ instead of $O(x^{1/2})$. Therefore, the side-condition is necessary.

We now show the proof of the theorem.

Proof. Firstly, we begin by considering the expression

$$\sum = \sum_n \omega(n) \left(\sum_{p \in \mathcal{P}} \left(\frac{n}{p} \right) \right)^2.$$

We note that each n is clearly counted with a non negative *weight*. Now, if $n = m^2$, then we have

$$\sum_{p \in \mathcal{P}} \left(\frac{n}{p} \right) = \sum_{p \in \mathcal{P}, p \nmid m} 1 \geq \mathcal{P} - \sum_{p \mid m} 1 \gg \mathcal{P}.$$

Now, note that

$$\sum_{p \mid m} 1 \ll \frac{\log m}{\log \log m} \implies \sum \gg \mathcal{P}^2 S(\mathcal{A}).$$

However, we also have

$$\sum = \sum_{p,q \in \mathcal{P}} \sum_n \omega(n) \left(\frac{n}{pq} \right) = \sum_{p \in \mathcal{P}} \sum_{n; p \mid n} \omega(n) + \sum_{p + q \in \mathcal{P}} \sum_n \omega(n) \left(\frac{n}{pq} \right)$$

$$\leq P\sum_{n}\omega(n)+\sum_{p+q\in\mathcal{P}}\sum_{n}\omega(n)\left(\frac{n}{pq}\right),$$

which completes our proof. ■

We now note an important corollary of the sieve.

Theorem 3.2 (Square Free Corollary)**.** *Let $E(n)=1$ if n is square-free, and $E(n)=0$ otherwise, then*

$$\sum_{n\leq x}E(n)E(n+1)=C\cdot x+O\left(x^{7/11}(\log x)^{7}\right),$$

where

$$C=\prod_{p}\left(1-2p^{-2}\right).$$

In order to demonstrate how the sieve works, we shall end up proving a weaker statement with error term $O(x^{2/3}\log(x)^3)$, which is still an improvement over the $O(x^{2/3+\varepsilon})$ error term which was discovered by Carlitz by a factor of x^{ε}.

Proof. First, begin by noting that

$$E(n)=\sum_{j^2|n}\mu(j),$$

where μ is the Mobius function. Now, we have

$$\sum_{n<x}E(n)E(n+1)=\sum_{j,k}\mu(j)\mu(k)N(x,j,k),$$

where

$$N(x,j,k)=\#\{n\leq x:j^2|n,k^2|n+1\}.$$

We note that $N(x,j,k)=xj^{-2}k^{-2}+O(1)$ if $\gcd(j,k)=1$, and 0 otherwise. We now estimate the contributions of terms $jk\leq y$ for some y which will be specified later. In particular, we note that the contributions are simply

$$\begin{aligned}&x\sum_{\substack{jk\leq y\\(j,k)=1}}\mu(j)\mu(k)(jk)^{-2}+O\left(\sum_{jk\leq y}1\right)\\&=x\sum_{(j,k)=1}\mu(jk)(jk)^{-2}+O\left(x\sum_{n>y}d(n)n^{-2}\right)+O\left(\sum_{n\leq y}d(n)\right)\\&=Cx+O\left(xy^{-1}\log y\right)+O(y\log y).\end{aligned}$$

where $d(n)$ is equivalent to σ_0, the number of divisors function. We also note that the remaining values of j,k lie in $O((\log(x)^2))$ ranges $J<j\leq 2J, K<k\leq 2K$, where

$$JK\gg y,\quad J,K\ll x^{1/2}.$$

Hence there exist some such, J,K for which

$$\sum_{jk}\mu(j)\mu(k)N(x,j,K)\ll N(\log(x))^2,$$

where

$$\sum_{jk>y} \mu(j)\mu(k)N(x,j,k) \ll N(\log x)^2$$

$$N = \#\left\{(j,k,u,v); J < j \le 2J, K < k \le 2K, j^2u+1 = k^2v \le x\right\}.$$

We will choose $x^{1/2} \le y \le x$, whence

$$\sum_{n<x} E(n)E(n+1) = Cx + O(y\log x) + O\left(N(\log x)^2\right). \tag{3.1}$$

Lastly, we have to bound N. We present the following bounds. We give an elementary bound

$$N \ll \sum_{K<k<2K} \sum_{u \le xJ^{-2}} \sum_{\substack{J<j\le 2J \\ j^2u \equiv -1 \pmod{k^2}}} 1.$$

Since this congruence condition has at most $\ll d(k)$ solutions $\bmod(k^2)$, the innermost sum is $\ll \left(1+JK^{-2}\right)d(k)$. Thus

$$N \ll xJ^{-2}\left(1+JK^{-2}\right)\sum_k d(k) \ll \left\{xKJ^{-2} + x(JK)^{-1}\right\}\log x \tag{3.2}$$

Now, WLOG, we assume that $J \gg K$, since the alternate case is more or less similar. Since $JK \gg y$, the bound 3.2 yields $N \ll xy^{-1/2}\log x$. On taking $y = x^{2/3}$ the estimate 3.1 would show that is true with the weaker error term $O\left(x^{2/3}(\log x)^3\right)$. This is already better than the result of Carlitz by an x^{ε} factor.

■

4. Applications of Square Sieve

4.1. **Sieves with Large Moduli.** In this section, we look at work done by Baier and Zhou (see [5], [6], [7]), and give an alternative proof of a theorem by them using Heath-Brown's square sieve, as covered by Baier [8].

Theorem 4.1 (Baier and Zhou). *Let $\varepsilon > 0$. Then for any $M \in \mathbb{Z}$, $N \in \mathbb{N}$, $Q \ge 1$ and sequence of complex numbers $(a_n)_{n\in\mathbb{Z}}$, we have*

$$\sum_{q\le Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q^2} \left|S\left(\frac{a}{q^2}\right)\right|^2 = O\left((NQ)^{\varepsilon}\left(Q^3 + N + \min\left\{N\sqrt{Q}, \sqrt{N}Q^2\right\}\right)Z\right), \tag{4.1}$$

where

$$S(\alpha) := \sum_{n=M+1}^{M+N} a_n e(n\alpha) \quad \textit{and} \quad Z := \sum_{n=M+1}^{M+N} |a_n|^2. \tag{4.2}$$

We note that 4.1 implies

$$\sum_{q\le Q} \sum_{\substack{a=1 \\ \gcd(a,q)=1}}^{q^2} \left|S\left(\frac{a}{q^2}\right)\right|^2 = O((NQ)^{\varepsilon}(Q^3 + N + \sqrt{N}Q^2)Z)$$

for some $\varepsilon > 0$. Now, we utilize 2.13 to obtain the following lemma.

Lemma 4.2. *Assume that $Q \geq 1, N \geq 1$ and $0 < \Delta \leq 1$. Then,*

$$\sum_{Q<q\leq 2Q} \sum_{\substack{a=1 \\ \gcd(a,q)=1}}^{q^2} \left| S\left(\frac{a}{q^2}\right)\right|^2 \ll \left(N + \Delta^{-1}\right) Z \cdot \max_{a\in\mathbb{R}} P(\alpha, \Delta),$$

where

$$P(a, \Delta) = \sum_{Q<q\leq 2Q} \sum_{\substack{a=1 \\ \gcd(a,q)=1 \\ |a/q^2-\alpha|\leq\Delta}}^{q^2} 1.$$

Now, in order to detect squares, we utilize 3.1. Dividing the q-range in (4.1) into dyadic intervals, it suffices to prove that

$$\sum_{Q<q\leq 2Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q^2} \left| S\left(\frac{a}{q^2}\right)\right|^2 = O\left((NQ)^{\varepsilon}\left(Q^3 + N + \sqrt{N}Q^2\right) Z\right). \tag{4.3}$$

We estimate $P(\alpha, \Delta)$ for any $\alpha \in \mathbb{R}$ and for $\Delta = \frac{1}{N}$ by dividing into two cases. Now, define the set of major arcs as

$$\mathcal{M} = \bigcup_{v\leq 1/(500Q^2\Delta)} \bigcup_{\substack{u=1 \\ \gcd(u,v)=1}}^{v} \left[\frac{u}{v} - \frac{1}{10Q^2v}, \frac{u}{v} + \frac{1}{10Q^2v}\right].$$

The case where $\alpha \in \mathcal{M}$ can be sorted directly by a Diophantine approximation, and therefore we resort to the case where $\alpha \in \mathbb{R} \setminus \mathcal{M}$.

We begin by noting that by Dirichlet's approximation theorem, there exist $(b, r) \in \mathbb{Z}^2$ such that

$$1 \leq r \leq 500Q^2 \quad \gcd(b, r) = 1 \quad \text{and} \quad \left|\frac{b}{r} - \alpha\right| \leq \frac{1}{500Q^2r}.$$

If $r \leq \frac{1}{500Q^2\Delta}$, it follows that $\alpha \in \mathcal{M}$. Thus, we have

$$\frac{1}{500Q^2\Delta} < r \leq 500Q^2 \quad \gcd(b, r) = 1, \quad \text{and} \quad \left|\frac{b}{r} - \alpha\right| \leq \Delta.$$

It follows that

$$P(\alpha, \Delta) \leq P\left(\frac{b}{r}, 2\Delta\right). \tag{4.4}$$

Let Φ_1 and Φ_2 be infinitely differentiable compactly supported functions from $\mathbb{R}$ to $\mathbb{R}^+$, supported in the intervals $[1/2, 5]$ and $[-10, 10]$ and bounded below by 1 on the intervals $[1, 4]$ and $[-4, 4]$, respectively. Then

$$P\left(\frac{b}{r}, 2\Delta\right) \ll \sum_{q\in\mathbb{Z}} \Phi_1\left(\frac{q^2}{Q^2}\right) \cdot \sum_{a\in\mathbb{Z}} \Phi_2\left(\frac{a - q^2b/r}{Q^2\Delta}\right). \tag{4.5}$$

Let

$$R > (QN)^{\varepsilon} \tag{4.6}$$

be a parameter, to be fixed later, and

$$\mathcal{P} := \{p \in \mathbb{P} \;:\; R < p \le 2R \text{ and } p \nmid r\}\,, \tag{4.7}$$

where $\mathbb{P}$ is the set of all primes. In the notation of Theorem 3.1, we have

$$P := \sharp\mathcal{P} = \pi(2R) - \pi(R) - \omega(r) \sim \frac{R}{\log R}. \tag{4.8}$$

Now applying the square sieve, Lemma 3.1, to the right-hand side of (4.5), we get

$$\begin{aligned} P\left(\frac{b}{r}, 2\Delta\right) \ll & \frac{1}{P} \cdot \sum_{n\in\mathbb{Z}} \Phi_1\left(\frac{n}{Q^2}\right) \cdot \sum_{a\in\mathbb{Z}} \Phi_2\left(\frac{a-nb/r}{Q^2\Delta}\right) + \\ & \frac{1}{P^2} \cdot \sum_{\substack{p_1,p_2\in\mathcal{P}\\ p_1\neq p_2}} \left| \sum_{n\in\mathbb{Z}} \Phi_1\left(\frac{n}{Q^2}\right) \cdot \left(\frac{n}{p_1p_2}\right) \cdot \sum_{a\in\mathbb{Z}} \Phi_2\left(\frac{a-bn/r}{Q^2\Delta}\right) \right|. \end{aligned} \tag{4.9}$$

Now, the RHS can be evaluated as follows.

$$\begin{aligned} & \sum_{n\in\mathbb{Z}} \Phi_1\left(\frac{n}{Q^2}\right) \cdot \sum_{a\in\mathbb{Z}} \Phi_2\left(\frac{a-nb/r}{Q^2\Delta}\right) \le \sum_{\substack{Q^2/2\le n\le 5Q^2\\ |a/n-b/r|\le 20\Delta}} \sum_{a\in\mathbb{Z}} 1 \\ = & \sum_{\substack{Q^2/2\le n\le 5Q^2\\ (a,n)\le 2500Q^4\Delta\\ |a/n-b/r|\le 20\Delta}} \sum_{a\in\mathbb{Z}} 1 + \sum_{\substack{Q^2/2\le n\le 5Q^2\\ (a,n)>2500Q^4\Delta\\ |a/n-b/r|\le 20\Delta}} \sum_{a\in\mathbb{Z}} 1 \\ \le & \sum_{d\le 2500Q^4\Delta} \sum_{\substack{Q^2/(2d)\le n_1\le 5Q^2/d\\ (a_1,n_1)=1\\ |a_1/n_1-b/r|\le 20\Delta}} \sum_{a_1\in\mathbb{Z}} 1 + \sum_{\substack{n_1\le 1/(500Q^2\Delta)\\ (a_1,n_1)=1\\ |a_1/n_1-b/r|\le 20\Delta}} \sum_{a_1\in\mathbb{Z}} \sum_{Q^2/(2n_1)\le d\le 5Q^2/n_1} 1. \end{aligned}$$

The rest of the proof utilizes a delicate Poisson Summation, which is beyond the scope of this paper. However, the application of the square sieve is apparent!

4.2. **Elliptic Curves.** In this section, we look at unexpected applications of the square sieve. In particular, we look at applications of the square sieve to elliptic curves and other algebraic varieties. First, we begin by stating the correspondence between binary cubic forms and elliptic curves, which was first discovered by Mordell. We give a sketch of the proof given by Bennett [9]

Theorem 4.3. *There exists a correspondence between the set of integral solutions* $S_k = \{(X_1,Y_1),\ldots,(X_{N_k},Y_{N_k})\}$ *for the Mordell equation* $Y^2 = X^3 + k$ *and the set* T_k *of triples* (F,x,y) *where* F *is a binary cubic form of the shape* $ax^3 + 3bx^2y + 3cxy^2 + dy^3$ *with discriminant* $-108k$ *and with integers* x, y *satisfying* $F(x,y) = 1$*. Furthermore, there exists a bijection between* T_k *and* S_k *under the actions of* $SL_2(\mathbb{Z})$ *and* $GL_2(\mathbb{Z})$*.*

Proof. Let

$$F = F(x,y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3$$

be a binary cubic form with the discriminant

$$D_F = -27(a^2d^2 - 6abcd - 3b^2c^2 + 4ac^3 + 4b^3d)$$

We observe the fact that the set of the binary cubic forms of the shape F is closed within the larger set of binary cubic forms of the set $Z[x, y]$ under the action of both SL_2 and GL_2. Now, describe the Hessian of the F to be

$$H = H_F(x, y) = -\frac{1}{4}\left(\frac{\partial^2 F}{\partial x^2}\frac{\partial^2 F}{\partial y^2} - \left(\frac{\partial^2 F}{\partial x \partial y}\right)^2\right)$$

and the Jacobian determinant of F and H, a cubic form $G = G_F$ defined as

$$G = G_F(x, y) = \frac{\partial F}{\partial x}\frac{\partial H}{\partial y} - \frac{\partial F}{\partial y}\frac{\partial H}{\partial x}.$$

Now, we have

$$H/9 = \left(b^2 - ac\right)x^2 + (bc - ad)xy + \left(c^2 - bd\right)y^2$$

and

$$G/27 = a_1x^3 + 3b_1x^2y + 3c_1xy^2 + d_1y^3,$$

where

$$a_1 = -a^2d+3abc-2b^3, \quad b_1 = -b^2c-abd+2ac^2, \quad c_1 = bc^2-2b^2d+acd, \quad d_1 = -3bcd+2c^3+ad^2.$$

These covariants satisfy the syzygy

$$4H(x, y)^3 = G(x, y)^2 + 27DF(x, y)^2.$$

Defining $D_1 = D/27, H_1 = H/9$ and $G_1 = G/27$, we get

$$4H_1(x, y)^3 = G_1(x, y)^2 + D_1F(x, y)^2.$$

We note that if (x_0, y_0) satisfies the equation $F(x_0, y_0) = 1$ and $D_1 \equiv 0(\mod 4)$ then necessarily $G_1(x_0, y_0) \equiv 0(\mod 2)$. We may therefore conclude that $Y^2 = X^3 + k$, where

$$X = H_1(x_0, y_0), \quad Y = \frac{G_1(x_0, y_0)}{2} \quad \text{and} \quad k = -\frac{D_1}{4} = -\frac{D}{108}.$$

It follows that, to a given triple (F, x_0, y_0), where F is a cubic form of the shape $ax^3 + 3bx^2y + 3cxy^2 + dy^3$ with discriminant $-108k$, and x_0, y_0 are integers for which $F(x_0, y_0) = 1$, we can associate an integral point on the Mordell equation $Y^2 = X^3 + k$. The converse of this can be proven easily by taking the covariants of the factors to be

$$X = \frac{G_1(1, 0)}{2} = \frac{G(1, 0)}{54} \text{ and } Y = H_1(1, 0) = \frac{H(1, 0)}{9}$$

The proof of bijection between T_k and S_k under the action of $GL_2(\mathbb{Z})$ and $SL_2(\mathbb{Z})$ is achieved by constructing a contradiction. ■

Now that we have constructed the bijection between binary cubic forms and elliptic curves, we note that the number of integral solutions for an elliptic curve of the form $E := y^2 = x^3+k$, denoted by $N(E) = O(h_3(k))$, where $h_3(k)$ is the class number of binary cubic forms with discriminant k, or alternatively, the 3 part of the class number of the quadratic field $\mathbb{Q}(\sqrt{k})$. Therefore, bounding $h_3(k)$ will allow us to bound the number of integral solutions on elliptic curves of the form $y^2 = x^3 + k$. In fact, the following lemma by Bennett proves a stronger statement by making the constant explicit.

Lemma 4.4. *If k is a nonzero integer, then the equation*

$$y^2 = x^3 + k$$

has at most $10h_3(-108k)$ solutions in integers x, y where $h_3(-108k)$ is the class number of the binary cubic forms with discriminant $-108k$, which is also referred to as the 3-part of class number of the quadratic field $\mathbb{Q}(\sqrt{-108k}) = \mathbb{Q}(\sqrt{-3k})$.

Now that we have made the relationship between Mordell curves and binary cubic forms explicit, we present an argument by Pierce [10], which shows that counting points on a cubic surface with certain constraints suffices to bound $h_3(k)$.

Theorem 4.5 (Pierce)**.** *Let d be a non-zero integer, then the* 3 *part of the class number of the quadratic field, $Q(\sqrt{d})$ admits the bound*

$$h_3(d) = O(d^{27/56+\varepsilon})$$

for all $\varepsilon > 0$.

We provide a partial sketch of the work done by Pierce [11]

First, we begin by reducing the problem of bounding $h_3(d)$ to counting integral solutions of a Diophantine equation with certain constraints, as shown below. Let d be a square-free positive integer. By the Scholz reflection principle $\log_3(h_3(-d))$ and $\log_3(h_3(+3d))$ differ by a bounded amount (indeed, they differ by at most one). Hence, we may restrict our attention to imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$. Suppose $[a] \in CL(-d)$ is a non-trivial element such that $[a]^3$ is the principal ideal class. By the Minkowski bound, there is an integral ideal b in $[a]$ with norm $\mathfrak{N}(b) \leq 2\sqrt{|\Delta|}/\pi$ where Δ is the discriminant of the field. Furthermore, since b^3 is principal, we may write $4(\mathfrak{N}(b))^3 = y^2 + dz^2$ for some $y, z \in \mathbb{N}$. Therefore, an integer point on the cubic surface

$$4x^3 = y^2 + dz^2$$

specifies at most $O(D^\varepsilon)$ ideals in ideals b, so we may obtain an upper bound for $h_3(-d)$ by counting the number of integer points on (3) in the region $x \leq L$, $y \leq M$, and $z \leq N$, where

$$L = \left(\frac{4}{\pi}\right) d^{1/2}, \quad M = \left(\frac{16}{\pi^{3/2}}\right) d^{3/4}, \quad N = \left(\frac{16}{\pi^{3/2}}\right) d^{1/4}. \tag{4.10}$$

We obtain a nontrivial bound for $h_3(-d)$ by counting the number of squares of the form

$$4x^3 - dx^2 \quad \text{with} \quad x \leq L,\ z \leq N.$$

Now, Pierce introduces the square sieve to deal with the above-mentioned question in a particularly interesting way.

Theorem 4.6 (Square Sieve Variant)**.** *Let $\mathcal{A} = \{uv : u \in \mathcal{U}, v \in \mathcal{V}\}$ where $\mathcal{U}$ and $\mathcal{V}$ are disjoint sets of primes. Let $A = \#\mathcal{A}, U = \#\mathcal{U}$, and $V = \#\mathcal{V}$. Suppose that $\omega(n) = 0$ for*

$n = 0$ *and for* $|n| \geq \exp(\min(U, V))$*. Then*

$$\sum_{n} \omega\left(n^2\right) \ll A^{-1} \sum_{n} \omega(n) + A^{-2} \sum_{\substack{f \neq g \in \mathcal{A} \\ (f,g)=1}} \left| \sum_{n} \omega(n) \left(\frac{n}{fg}\right) \right|$$

$$+ V A^{-2} \sum_{u \neq u' \in \mathcal{U}} \left| \sum_{n} \omega(n) \left(\frac{n}{uu'}\right) \right| + A^{-2} |E(\mathcal{U})|$$

$$+ U A^{-2} \sum_{v \neq v' \in \mathcal{V}} \left| \sum_{n} \omega(n) \left(\frac{n}{vv'}\right) \right| + A^{-2} |E(\mathcal{V})|.$$

The error terms $E(\mathcal{U})$ *and* $E(\mathcal{V})$ *are defined by:*

$$E(\mathcal{U}) = \sum_{v \in \mathcal{V}} \sum_{u \neq u' \in \mathcal{U}} \sum_{\substack{n \\ v \mid n}} \omega(n) \left(\frac{n}{uu'}\right),$$

$$E(\mathcal{V}) = \sum_{u \in \mathcal{U}} \sum_{v \neq v' \in \mathcal{V}} \sum_{\substack{n \\ u \mid n}} \omega(n) \left(\frac{n}{vv'}\right).$$

Proof.

$$\Sigma = \sum_{n} \omega(n) \left(\sum_{f \in \mathcal{A}} \left(\frac{n}{f}\right) \right)^2$$

Each n is summed with non-negative weight, and in particular, if $n = m^2$, then

$$\sum_{f \in \mathcal{A}} \left(\frac{n}{f}\right) = \sum_{f \in \mathcal{A}} \left(\frac{m^2}{f}\right) = \sum_{\substack{f \in \mathcal{A} \\ (f,m)=1}} 1 \geq A - \sum_{\substack{f \in \mathcal{A} \\ (f,m) \neq 1}} 1 \gg A$$

since $\omega(n) = 0$ for $|n| \geq \exp(\min(U, V))$. Thus

$$\Sigma \gg A^2 \sum_{n} \omega\left(n^2\right) \tag{4.11}$$

But also

$$\Sigma = \sum_{f,g \in \mathcal{A}} \sum_{n} \omega(n) \left(\frac{n}{fg}\right)$$

$$= \sum_{f \in \mathcal{A}} \sum_{n} \omega(n) \left(\frac{n}{f^2}\right) + \sum_{\substack{f \neq g \in \mathcal{A} \\ (f,g)=1}} \sum_{n} \omega(n) \left(\frac{n}{fg}\right)$$

$$+ \sum_{\substack{f \neq g \in \mathcal{A} \\ (f,g) \neq 1}} \sum_{n} \omega(n) \left(\frac{n}{fg}\right).$$

The last term mentioned above may be broken into the two terms

$$S(\mathcal{U})+S(\mathcal{V})=\sum_{v\in\mathcal{V}}\sum_{u\neq u'\in\mathcal{U}}\sum_{\substack{n\\ v\nmid n}}\omega(n)\left(\frac{n}{uu'}\right)+\sum_{u\in\mathcal{U}}\sum_{v\neq v'\in\mathcal{V}}\sum_{\substack{n\\ u\nmid n}}\omega(n)\left(\frac{n}{vv'}\right).$$

Furthermore, $S(\mathcal{U})$ may be written as a main term $M(\mathcal{U})$, minus a correction term $E(\mathcal{U})$

$$S(\mathcal{U})=M(\mathcal{U})-E(\mathcal{U})=V\sum_{u\neq u'\in\mathcal{U}}\sum_{n}\omega(n)\left(\frac{n}{uu'}\right)-\sum_{v\in\mathcal{V}}\sum_{u\neq u'\in\mathcal{U}}\sum_{\substack{n\\ v|n}}\omega(n)\left(\frac{n}{uu'}\right).$$

Analogously, we may write $S(\mathcal{V})=M(\mathcal{V})-E(\mathcal{V})$. Thus, we have the Σ inequality.

$$\begin{aligned}|\Sigma| \ll & A\sum_{n}\omega(n)+\sum_{\substack{f\neq g\in\mathcal{A}\\ (f,g)=1}}\left|\sum_{n}\omega(n)\left(\frac{n}{fg}\right)\right|\\ &+V\sum_{u\neq u'\in\mathcal{U}}\left|\sum_{n}\omega(n)\left(\frac{n}{uu'}\right)\right|+|E(\mathcal{U})|\\ &+U\sum_{v\neq v'\in\mathcal{V}}\left|\sum_{n}\omega(n)\left(\frac{n}{vv'}\right)\right|+|E(\mathcal{V})|.\end{aligned}$$

The result then follows by comparison with 4.11. ■

Now, let

$$T(d)=\#\left\{x,y,z\in\mathbb{N}:y^2=4x^3-dz^2:x\leq L,y\leq M,z\leq N\right\},$$

where L,M,N are as defined in 4.10. Then

$$h_3(-d)\ll d^{\epsilon}T(d).$$

Furthermore, let

$$\omega(n)=\#\left\{x,z\in\mathbb{N}:n=4x^3-dz^2:x\leq L,z\leq N\right\},$$

such that

$$T(d)=\sum_{n=1}^{\infty}\omega\left(n^2\right).$$

Therefore, if we obtain nontrivial bound $T(d)\ll d^{1/2-\theta}$, for some constant $\theta>0$, we will obtain a nontrivial bound on $h_3(d)$. The abovementioned excursion shows the utility of the square sieve!

References

[1] Gallagher P. A larger sieve. Acta Arithmetica. 1971;18(1):77-81. Available from: `http://eudml.org/doc/205009`.

[2] Davenport H, Montgomery HL. Multiplicative Number Theory. Graduate Texts in Mathematics. Springer New York; 2013. Available from: `https://books.google.co.in/books?id=SFztBwAAQBAJ`.

[3] Montgomery HL. Topics in Multiplicative Number Theory. Lecture notes in mathematics. University of Cambridge; 1971. Available from: `https://books.google.co.in/books?id=j256AQAACAAJ`.

[4] Heath-Brown DR. The Square Sieve and Consecutive Square-Free Numbers. Mathematische Annalen. 1984;266:251-60. Available from: `http://eudml.org/doc/163852`.

[5] Baier S. On the large sieve with sparse sets of moduli. J Ramanujan Math Soc. 2006;21(3):279-95.

[6] Baier S, Zhao L. An improvement for the large sieve for square moduli. J Number Theory. 2008;128(1):154-74.

[7] Zhao L. Large sieve inequality with characters to square moduli. Acta Arith. 2004;112(3):297-308.

[8] Baier S. The square sieve and the large sieve with square moduli; 2016.

[9] Bennett MA, Ghadermarzi A. Mordell's equation: a classical approach. LMS Journal of Computation and Mathematics. 2015;18(1):633–646.

[10] Pierce LB. A bound for the 3-part of class numbers of quadratic fields by means of the square sieve. Forum Mathematicum. 2006;18(4):677-98. Available from: `https://doi.org/10.1515/FORUM.2006.034` [cited 2024-06-09].

[11] Pierce LB. The 3-part of Class Numbers of Quadratic Fields. Journal of the London Mathematical Society. 2005 06;71(3):579-98. Available from: `https://doi.org/10.1112/S002461070500637X`.

Email address: `navvye.anand@caltech.edu`